

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-44356

(P2002-44356A)

(43)公開日 平成14年2月8日(2002.2.8)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコト(参考)
H 04 N 1/00	1 0 7	H 04 N 1/00	1 0 7 Z 5 B 0 5 7
G 06 F 15/00	3 3 0	G 06 F 15/00	3 3 0 A 5 B 0 8 5
G 06 T 1/00	5 0 0	G 06 T 1/00	5 0 0 B 5 C 0 6 2
H 04 N 1/387		H 04 N 1/387	5 C 0 7 5
1/44		1/44	5 C 0 7 6

審査請求 未請求 請求項の数9 OL (全 19 頁)

(21)出願番号 特願2000-224096(P2000-224096)

(22)出願日 平成12年7月25日(2000.7.25)

(71)出願人 000005049

シャープ株式会社

大阪府大阪市阿倍野区長池町22番22号

(72)発明者 西 明宏

大阪府大阪市阿倍野区長池町22番22号 シ  
ャープ株式会社内

(72)発明者 木村 正邦

大阪府大阪市阿倍野区長池町22番22号 シ  
ャープ株式会社内

(74)代理人 100075502

弁理士 倉内 義朗

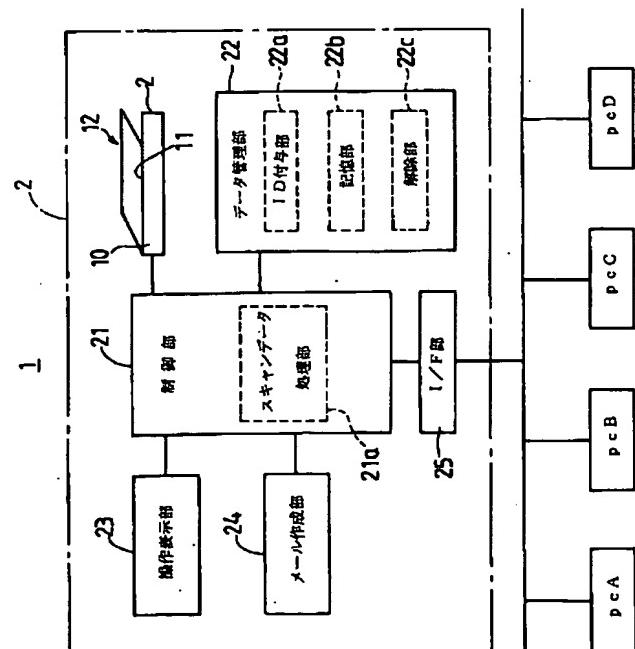
最終頁に続く

(54)【発明の名称】スキャナ装置

(57)【要約】

【課題】機密レベルごとに異なるIDを複数のパソコン用コンピュータに対し付与することで、各パソコン用コンピュータにおいて機密レベルに応じたスキャンデータを共有可能とするスキャナ装置を提供する。

【解決手段】LANに接続され、スキャンデータを複数のパソコン用コンピュータpcA～pcDに対しダウンロード可能に出力するスキャナ装置1として、階層の異なる機密レベルを設定し、その各機密レベルに応じたIDをそれぞれパソコン用コンピュータに対し付与するID付与部22aと、機密レベルに応じた画像処理をそれぞれスキャンデータに施すスキャンデータ処理部21aとを備え、スキャンデータ処理部によりそれぞれ画像処理された階層の異なるスキャンデータを、各階層の機密レベルに応じたパソコン用コンピュータに対しそれぞれダウンロード可能に出力し、ネットワークで共用する。



(2)

1

## 【特許請求の範囲】

【請求項1】 複数のネットワーク端末を備えたネットワークに接続され、原稿台上的原稿をスキャンしたスキャンデータを各ネットワーク端末に対しダウンロード可能に出力するスキャナ装置において、  
スキャンデータに対し階層の異なる機密レベルを設定し、その各機密レベルに応じたIDをそれぞれネットワーク端末に対し付与するID付与手段と、  
このID付与手段により付与された機密レベルに応じた画像処理をそれぞれスキャンデータに施す画像処理手段とを備え、  
上記画像処理手段によりそれぞれ画像処理されたスキャンデータを、ID付与手段により付与された機密レベルに応じたネットワーク端末に対しそれぞれダウンロード可能に出力するようになされていることを特徴とするスキャナ装置。

【請求項2】 上記請求項1に記載のスキャナ装置において、  
画像処理手段は、上階層の機密レベルのスキャンデータに対し原稿の色情報を変更することによって下階層の機密レベルの画像処理が施されるようになされていることを特徴とするスキャナ装置。

【請求項3】 上記請求項1に記載のスキャナ装置において、  
画像処理手段は、上階層の機密レベルのスキャンデータに対し原稿の特定部分の文字データ情報を削除することによって下階層の機密レベルの画像処理が施されるようになされていることを特徴とするスキャナ装置。

【請求項4】 上記請求項1に記載のスキャナ装置において、  
画像処理手段は、上階層の機密レベルのスキャンデータに対し原稿の解像度を低くすることによって下階層の機密レベルの画像処理が施されるようになされていることを特徴とするスキャナ装置。

【請求項5】 上記請求項1に記載のスキャナ装置において、  
画像処理手段は、上階層の機密レベルのスキャンデータに対し原稿の特定部分にウォーターマークを挿入することによって下階層の機密レベルの画像処理が施されるようになされていることを特徴とするスキャナ装置。

【請求項6】 上記請求項1に記載のスキャナ装置において、

画像処理手段は、複数枚の原稿からなるスキャンデータに対し上階層の機密レベルとなるページを削除することによって下階層の機密レベルの画像処理が施されるようになされていることを特徴とするスキャナ装置。

【請求項7】 請求項1に記載のスキャナ装置において、  
下階層の機密レベルの画像処理が施されたスキャンデータを上階層の機密レベルに応じた画像処理に変更するよ

2

うに機密レベルの設定を上位の階層へ移行可能に解除する解除手段を備えていることを特徴とするスキャナ装置。

【請求項8】 請求項7に記載のスキャナ装置において、  
解除手段は、機密レベルの設定解除が特定のID解除キーを入力することによって行われるようになされており、

この特定のID解除キーは、下階層の機密レベルに応じたネットワーク端末に対しネットワークを介して送信されるようになされていることを特徴とするスキャナ装置。

【請求項9】 請求項7に記載のスキャナ装置において、

解除手段は、機密レベルの設定解除が特定のID解除キーを入力することによって行われるようになされており、

この特定のID解除キーは、スキャナ装置本体の表示部に表示されるようになされていることを特徴とするスキャナ装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】 本発明は、複数のネットワーク端末を備えたネットワークに接続されるスキャナ装置に関し、詳しくは、各ネットワーク端末に対し階層の異なる機密レベルを設定し、その機密レベルに応じてスキャンデータをダウンロードすることによって、スキャンされる原稿の機密性および著作権などを保護する対策に係わる。

## 【0002】

【従来の技術】 従来より、例えば特開平10-233880号公報に開示されるように、画像データの入力手段として用いられるスキャナ装置を、ネットワークに接続し、原稿台上的原稿をスキャンしたスキャンデータ（画像データ）を複数のネットワーク端末に対しダウンロード可能に出力するようにしたもののが知られている。そして、このスキャナ装置では、スキャンデータにネットワーク端末の特定のIDとスキャンデータの名前とを付与することによって、ネットワーク上においてダウンロード可能なネットワーク端末を特定し、スキャンデータのダウンロードに制限を加えることで、スキャンデータの機密性を確保するようになされている。

## 【0003】

【発明が解決しようとする課題】 ところが、上記従来のものでは、特定のIDをもたないネットワーク端末にあっては、スキャナ装置によりスキャンしたスキャンデータをダウンロードつまり共有することができず、ネットワーク上で予め設定された特定のネットワーク端末でしかスキャンデータを共有することができない。

【0004】 このため、スキャンデータの共有はその全

50

(3)

3

てか否かしかなく、スキャンデータの一部分のみを機密とする場合においても、特定のIDをもたないネットワーク端末では、その一部分（機密部分）を除くスキャンデータをネットワーク上で共有することができず、機密に触れない必要最小限の情報でさえも共有することができないことになる。

【0005】本発明はかかる点に鑑みてなされたものであり、その目的とするところは、機密レベルごとに異なるIDを複数のネットワーク端末に対し付与することで、各ネットワーク端末において機密レベルに応じたスキャンデータを共有することができるスキャナ装置を提供することにある。

【0006】

【課題を解決するための手段】上記目的を達成するためには、本発明は、複数のネットワーク端末を備えたネットワークに接続され、原稿台上的原稿をスキャンしたスキャンデータを各ネットワーク端末に対しダウンロード可能に出力するスキャナ装置を前提とする。そして、階層の異なる機密レベルを設定し、その各機密レベルに応じたIDをそれぞれネットワーク端末に対し付与するID付与手段と、このID付与手段により付与された機密レベルに応じた画像処理をそれぞれスキャンデータに施す画像処理手段とを備え、上記画像処理手段によりそれぞれ画像処理されたスキャンデータを、ID付与手段により付与された機密レベルに応じたネットワーク端末に対しそれぞれダウンロード可能に出力するようにしている。

【0007】この特定事項により、スキャンデータの一部分のみを機密とする場合、階層の異なる機密レベルに応じたIDがそれぞれ付与されたネットワーク端末では、機密レベルに応じた画像処理をそれぞれ施したスキャンデータがネットワーク上で共有されることになる。これにより、下階層の機密レベルのネットワーク端末では、上階層の機密レベルの機密部分を除くスキャンデータがネットワーク上で共有され、上階層の機密に触れない下階層の機密レベル（必要最小限の情報）のスキャンデータを共有することが可能となる。

【0008】一方、上階層の機密レベルのスキャンデータは、その上階層の機密レベルに応じたIDが付与されたネットワーク端末においてのみ共有され、そのスキャンデータの機密性および著作権を円滑に保護することが可能となる。

【0009】特に、下階層のスキャンデータに対する画像処理の具体的な施し方としては、以下の構成が掲げられる。

【0010】つまり、下階層の機密レベルのスキャンデータに対し原稿の色情報を変更する画像処理を画像処理手段によって施すようにしている。

【0011】この特定事項により、下階層の機密レベルのIDが付与されたネットワーク端末では、原画をたと

(4)

4

えばカラーからモノクロに変更することも可能となり、このようにモノクロに変更したスキャンデータが共有され、上階層の機密レベルとなる原画の機密性および著作権が円滑に保護される上、スキャンデータのデータ量が少なくなってダウンロードを高速で行うことが可能となる。

【0012】これに対し、下階層の機密レベルのスキャンデータに対し原稿の特定部分の文字データ情報を削除する画像処理を画像処理手段によって施すようにした場合には、下階層の機密レベルのIDが付与されたネットワーク端末では、たとえば住所、氏名、電話番号などの文字データ情報を削除することも可能となり、このように悪用され易い文字データ情報を削除したスキャンデータが共有され、上階層の機密レベルとなる住所、氏名、電話番号などの知られたくない文字データ情報の機密性が円滑に保護されることになる。

【0013】また、下階層の機密レベルのスキャンデータに対し原稿の解像度を低くする画像処理を画像処理手段によって施すようにした場合には、下階層の機密レベルのIDが付与されたネットワーク端末では、原画の解像度を低くしたスキャンデータが共有され、上階層の機密レベルとなる原画の機密性および著作権が円滑に保護される上、スキャンデータのデータ量が少なくなってダウンロードを高速で行うことが可能となる。

【0014】しかも、下階層の機密レベルのスキャンデータに対し原稿の特定部分にウォータマークを挿入する画像処理を画像処理手段によって施すようにした場合には、下階層の機密レベルのIDが付与されたネットワーク端末では、たとえば社外秘などのウォータマークを挿入することも可能となり、このようなウォータマークを挿入したスキャンデータが共有され、ダウンロードした社外秘付きの原稿に対し個人レベルで機密性が喚起され、上階層の機密レベルとなる原稿の機密性および著作権が各人によって保護されることになる。

【0015】さらに、複数枚の原稿からなるスキャンデータに対し上階層の機密レベルとなるページを削除する画像処理を画像処理手段によって施すようにした場合には、下階層の機密レベルのIDが付与されたネットワーク端末では、下階層の機密レベルのページのみとなるスキャンデータが共有され、上階層の機密レベルとなる原稿の機密性が円滑に保護される上、スキャンデータのデータ量が少なくなってダウンロードを高速で行うことが可能となる。

【0016】特に、下層階の機密レベルのスキャンデータから上位の機密レベルのスキャンデータを取得可能とするものとして、以下の構成が掲げられる。

【0017】つまり、下階層の機密レベルに応じて画像処理が施されたスキャンデータを上階層の機密レベルに応じた画像処理に変更するように機密レベルの設定を上位の階層へ移行可能に解除する解除手段を備えている。

(4)

5

【0018】この特定事項により、下階層の機密レベルのIDが付与されたネットワーク端末において、解除手段により機密レベルの設定を上位の階層へ移行可能に解除することで、たとえば原画などの所望の情報が取り出され、必要に応じて上位階層の機密レベルのスキャンデータを共有することが可能となる。

【0019】特に、機密レベルを上位へ移行可能に解除する具体的な設定の仕方としては、以下の構成が掲げられる。

【0020】つまり、特定のID解除キーを入力することによって解除手段による機密レベルの設定解除を行えるようにし、この特定のID解除キーを、下階層の機密レベルに応じたネットワーク端末に対しネットワークを介して送信するようにしている。

【0021】この特定事項により、下階層の機密レベルのIDが付与されたネットワーク端末において、ネットワークを介して送信された特定のID解除キーを入力することで、たとえば原画などの所望の情報が取り出され、必要に応じて上位階層の機密レベルのスキャンデータを共有することが可能となる。しかも、取得した上位階層の機密レベルのスキャンデータを、再び他のネットワーク端末に対し制限を加えた状態、つまり下階層の機密レベルのIDを付与した状態で、ダウンロード可能に出力することが行える。

【0022】これに対し、特定のID解除キーを入力することによって解除手段による機密レベルの設定解除を行えるようにし、この特定のID解除キーを、スキャナ装置本体の表示部に表示するようにした場合には、下階層の機密レベルのIDが付与されたネットワーク端末において、スキャナ装置本体の表示部に表示された特定のID解除キーを入力することで、必要に応じて原画などの所望の情報（上位階層の機密レベルのスキャンデータ）を共有することが可能となる上、他のネットワーク端末に対し下階層の機密レベルのIDを付与してダウンロード可能に出力することが可能となる。

【0023】

【発明の実施の形態】以下、本発明の実施の形態を図面に基づいて説明する。

【0024】図1は、本発明の実施形態に係わるスキャナ部を備えたスキャナ装置を示し、このスキャナ装置1は、ネットワーク端末としての4台のパーソナルコンピュータp c A～p c Dを備えたLAN（ネットワーク）に接続され、原稿台11上の原稿をスキャンしたスキャンデータを各パーソナルコンピュータp c A～p c Dに対しダウンロード可能に出力するようになされている。この場合、スキャナ部12によりスキャンされたスキャンデータは、スキャナ部本体10（スキャナ装置本体）内の記憶部（図示せず）に記憶されている。

【0025】スキャナ装置1には、コントロールボックス2が設けられている。このコントロールボックス2

6

は、スキャナ部12の動作を制御する制御部21を備えている。そして、コントロールボックス2には、スキャンデータの機密レベルに応じた階層ごとのデータを管理するデータ管理部22と、データ管理部22に対し必要なデータを操作する操作表示部23と、各パーソナルコンピュータp c A～p c Dに対しそれぞれeメールを作成するメール作成部24と、スキャナ装置1外部のパーソナルコンピュータp c A～p c Dなどに対しスキャンデータを入出力可能とするインターフェイス部25（以降、I/F部と称する）と、これら各部に対して電力を供給する電源ユニット（図示せず）とが収容されている。そして、データ管理部22、操作表示部23、メール作成部24およびI/F部25は、制御部21に対し信号が入出力可能となるように接続されている。

【0026】データ管理部22は、階層の異なる機密レベルを設定するものであって、その各階層の機密レベルに応じたIDコードをそれぞれパーソナルコンピュータp c A～p c Dに対し付与するID付与手段としてのID付与部22aと、このID付与部22aにより付与された機密レベルに応じた画像処理の内容（手法）を記憶する記憶部22bとを備えている。この記憶部22bには、上階層の機密レベルのスキャンデータに対し原稿の色情報をカラーからモノクロに変更して下階層の機密レベルの画像処理を施す手法と、上階層の機密レベルのスキャンデータに対し原稿の特定部分の電話番号およびメールアドレスなどの文字データ情報を削除して下階層の機密レベルの画像処理を施す手法と、上階層の機密レベルのスキャンデータに対し原稿の解像度を1200dpiから600dpiまで低くして下階層の機密レベルの画像処理を施す手法と、スキャンデータに対し上階層の機密レベルの原稿の特定部分に社外秘などのウォータマークを挿入して下階層の機密レベルの画像処理を施す手法と、複数枚の原稿からなるスキャンデータに対し上階層の機密レベルとなるページを削除して下階層の機密レベルのページのみとするページ制御の画像処理を施す手法とが記憶されている。

【0027】また、データ管理部22は、下階層の機密レベルに応じて画像処理が施されたスキャンデータを上階層の機密レベルに応じた画像処理に変更するように機密レベルの設定を上位の階層へ移行可能に解除する解除部22cを備えている。この解除部22cでは、機密レベルの設定解除が特定のID解除キーコードを入力することによって行われるようになされており、この特定のID解除キーコードは、下階層の機密レベルに応じたパーソナルコンピュータに対しLANを介してeメールで送信されるようになされている。

【0028】操作表示部23は、表示部としての液晶モニタ画面23a（図3参照）を備え、この液晶モニタ画面23a上において、データ管理部22の記憶部22bに記憶されている画像処理の内容を指示するようになさ

(5)

7

れている。

【0029】メール作成部24は、データ管理部22のID付与部22aにより付与された機密レベルに応じたIDコードの通りのパーソナルコンピュータp c A～p c D宛にeメールを作成するようになされている。

【0030】制御部21は、ID付与部22aにより付与された機密レベルに応じた画像処理をそれぞれスキャンデータに施す画像処理手段としてのスキャンデータ処理部21aを備えている。このスキャンデータ処理部21aでは、操作表示部23の液晶モニタ画面23a上において指示された画像処理の手法をデータ管理部22の記憶部22bから選択し、その選択された画像処理の内容に応じた処理をスキャンデータに対しそれぞれ施すことが行われる。

【0031】次に、パーソナルコンピュータp c A～p c Dに対しそれぞれの階層に見合ったスキャンデータを送信する際の制御部21による制御の手順を図2～図14の説明図、および図15～図19のフローチャートに基づいて説明する。この場合、上階層の機密レベルに応じたIDAがパーソナルコンピュータp c A, p c B, p c Dに付与され、下階層の機密レベルに応じたIDBがパーソナルコンピュータp c Cに付与されるものとする。

【0032】～スキャンデータSCDAT1を記憶する場合の説明～

先ず、スキャナ装置1においてスキャンしたスキャンデータSCDAT1をスキャナ部12の記憶部に記憶する場合には、図15のフローチャートのステップSA1において、原稿台11上の原稿をスキャンした後、ステップSA2で、機密レベルに応じたIDコードが、上記ステップSA1でスキャンしたスキャンデータに対しデータ管理部22のID付与部22aによって付与されているか否かを判定する。このとき、スキャンデータにはファイルネームとしてSCDAT1が付与される。

【0033】このステップSA2の判定が、IDコードを付与したスキャンデータSCDAT1（ファイルネーム）であるYESの場合には、ステップSA3において、操作表示部23の液晶モニタ画面23a上において指示された画像処理の手法をデータ管理部22の記憶部22bから選択する。この場合、操作表示部23の液晶モニタ画面23a上において、スキャンデータSCDAT1に対し上階層の機密レベルの原稿の特定部分に社外秘などのウォータマークを挿入して下階層の機密レベルの画像処理を施す手法と、4枚の原稿からなるスキャンデータSCDAT1に対し上階層の機密レベルとなるページを削除して下階層の機密レベルのページのみとするページ制御の画像処理を施す手法とが指示され、この指示に従いスキャンデータ管理部21aによってデータ管理部22の記憶部22bから選択される。

【0034】具体的には、図2に示すように、スキャン

8

データSCDAT1は、4枚の原稿からなるものであり、そのうち、第1ページ、第2ページおよび第4ページが上階層の機密レベルAとされる一方、第3ページが下階層の機密レベルBとされているので、上階層の機密レベルAから第1ページ、第2ページおよび第4ページを削除して下階層の機密レベルBの第3ページのみとするページ制御の画像処理がスキャンデータSCDAT1に施されることになる。従って、図3に示すように、操作表示部23の液晶モニタ画面23a上において、スキャンデータSCDAT1に対しページ制御の画像処理を施す操作を行う。つまり、第1ページ、第2ページおよび第4ページを上階層機密レベルAに、第3ページを下階層機密レベルA, B（上階層機密レベルAも含まれる）にそれぞれ設定する。

【0035】そして、図4に示すように、データ管理部22のID付与部22aによって、スキャンデータSCDAT1の各階層の機密レベルA, Bに応じたIDコード（ID）をそれぞれパーソナルコンピュータp c A～p c Dに対し付与する。具体的には、上階層の機密レベルAに応じたIDAコードとして「×××〇〇〇」をパーソナルコンピュータp c A, p c B, p c Dに、下階層の機密レベルBに応じたIDBコードとして「〇×〇×〇×」をパーソナルコンピュータp c Cにそれぞれ付与する。

【0036】その後、ステップSA4において、ヘッダー登録する。具体的には、図5に示すように、データ名としてのスキャンデータSCDAT1、各階層の機密レベルA, B、各階層の機密レベルA, Bに応じて付与されるIDAコード、IDBコード、および各階層の機密レベルA, Bに応じたIDコード通りに作成されたパーソナルコンピュータp c A～p c D宛のeメールアドレスをヘッダーとして登録する。また、図6に示すように、上階層機密レベルAではページ制御の画像処理を第1ページ～第4ページに施さないことを、下階層機密レベルBではページ制御の画像処理を第3ページにのみ施さないことをヘッダとして登録する。

【0037】しかる後、ステップSA5において、スキャンデータSCDAT1、各階層の機密レベルA, B、各階層の機密レベルA, Bに応じたIDAコード、IDBコード、およびIDコード通りに作成されたパーソナルコンピュータp c A～p c D宛のeメールアドレスなどのデータをスキャナ部本体10内の記憶部に記憶する。一方、上記ステップSA2の判定が、IDコードを付与したスキャンデータSCDAT1（ファイルネーム）でないNOの場合には、ステップSA6において、IDコードが付与されていないスキャンデータを記憶する。

【0038】そして、ステップSA6で、スキャンデータSCDAT1の終了指示があるか否かを判定し、スキャン終了の指示がなければ、ステップSA1に戻って、

(6)

9

原稿台11上の原稿をスキャンする。

【0039】ースキャンデータSCDAT2を引き続いで記憶する場合の説明一

スキャナ装置1においてスキャンしたスキャンデータSCDAT2もスキャナ部12の記憶部に記憶する場合には、図16のフローチャートのステップSB1において、原稿台11上の原稿をスキャンした後、ステップSB2で、機密レベルに応じたIDコードが、上記ステップSB1でスキャンしたスキャンデータに対しデータ管理部22のID付与部22aによって付与されているか否かを判定する。このとき、スキャンデータにはファイル名としてSCDAT2が付与される。

【0040】このステップSB2の判定が、IDコードを付与したスキャンデータSCDAT2(ファイル名)であるYESの場合には、ステップSB3において、操作表示部23の液晶モニタ画面23a上において指示された画像処理の手法をデータ管理部22の記憶部22bから選択する。この場合、操作表示部23の液晶モニタ画面23a上において、スキャンデータSCDAT2に対し上階層の機密レベルの原稿の特定部分の電話番号およびメールアドレスなどの文字データ情報を削除して下階層の機密レベルの画像処理を施す手法が指示され、この指示に従いスキャンデータ管理部21aによってデータ管理部22の記憶部22bから選択される。

【0041】具体的には、図7に示すように、スキャンデータSCDAT2は、社員固有のデータであり、そのうち、住所、氏名、電話番号およびeメールアドレスを全て備えたものが上階層の機密レベルAとされる一方、図8に示すように、その社員固有のデータから電話番号およびeメールアドレスを削除する画像処理が下階層の機密レベルBとしてスキャンデータSCDAT2に施されることになる。従って、操作表示部23の液晶モニタ画面23a上において、スキャンデータSCDAT2に対し電話番号およびeメールアドレスの文字情報を削除するように画像処理を施す操作を行う。

【0042】そして、図9に示すように、データ管理部22のID付与部22aによって、スキャンデータSCDAT2の各階層の機密レベルA、Bに応じたIDコード(ID)をそれぞれパーソナルコンピュータpca～pcDに対し付与する。具体的には、上階層の機密レベルに応じたIDAコードとして「×〇〇〇〇〇」を、下階層の機密レベルに応じたIDBコードとして「〇〇××××」をそれぞれパーソナルコンピュータpca～pcDに対し付与する。

【0043】それから、ステップSB4において、データ管理部22の解除部22cによって、下階層の機密レベルBに応じて画像処理が施されたスキャンデータSCDAT2を上階層の機密レベルAに応じた画像処理に変更する特定のID解除キーコードを登録するか否かを判定する。このステップSB4の判定が、特定のID解除

(6)

10

キーコードを登録するYESの場合には、ステップSB5において、下階層の機密レベルのIDBに対するID解除キーコードを登録する。

【0044】その後、上記ステップSB4の判定が特定のID解除キーコードを登録しないNOの場合と同様に、ステップSB6において、各階層の機密レベルA、Bに応じたパーソナルコンピュータpca～pcDのeメールアドレスを選択し、ステップSB7で、ヘッダー登録する。具体的には、図10に示すように、データ名としてのスキャンデータSCDAT2、各階層の機密レベルA、B、各階層の機密レベルA、Bに応じて付与されるIDAコード、IDBコード、機密レベルBの設定を上階層の機密レベルAへ移行可能に解除する特定のID解除キーコード、および各階層の機密レベルA、Bに応じたIDコード通りに作成されたパーソナルコンピュータpca～pcD宛のeメールアドレスをヘッダーとして登録する。また、図11に示すように、上階層機密レベルAではスキャンデータSCDAT2に対する画像処理を施さないことを、下階層機密レベルBでは電話番号およびeメールアドレスの文字情報を削除する画像処理を施すことをヘッダとして登録する。

【0045】しかる後、ステップSB8において、スキャンデータSCDAT2、各パーソナルコンピュータpca～pcD宛のeメールアドレス、およびヘッダなどのデータをスキャナ部本体10内の記憶部に記憶する。一方、上記ステップSB2の判定が、IDコードを付与したスキャンデータSCDAT2(ファイル名)でないNOの場合には、ステップSB8において、IDコードが付与されていないスキャンデータSCDAT2を記憶する。

【0046】それから、ステップSB9において、図12に示すように、データ管理部22のID付与部22aにより付与された機密レベルA、Bに応じたIDコード通りのパーソナルコンピュータpca～pcD宛のeメールをメール作成部24によって作成し、パーソナルコンピュータpca～pcD宛にそれぞれIDAコード、IDBコードをeメールで送信する。このとき、上述したスキャンデータSCDAT1を記憶する場合のフローチャートのステップSA5においてスキャナ部本体10内の記憶部に記憶された、スキャンデータSCDAT1の各階層の機密レベルA、Bに応じたIDAコード、IDBコード通りに、パーソナルコンピュータpca～pcD宛のeメールアドレスをメール作成部24によって作成し、パーソナルコンピュータpca～pcD宛にそれぞれIDAコード、IDBコードをeメールで送信する。

【0047】そして、ステップSB10で、スキャンデータSCDAT2の終了指示があるか否かを判定し、スキャン終了の指示がなければ、ステップSB1に戻つて、原稿台11上の原稿をスキャンする。

(7)

11

【0048】ースキャンデータSCDAT1に特定のID解除キーコードを付与する場合の説明ー

スキャンデータSCDAT1に対し後から特定のID解除キーコードを付与する場合には、先ず、図17のフローチャートのステップSC1において、予めIDコードが付与されているスキャンデータSCDAT1, SCDAT2のなかから、スキャンデータSCDAT1のファイルを選択する。

【0049】次いで、ステップSC2において、データ管理部22の解除部22cによって、下階層の機密レベルBに応じて画像処理が施されたスキャンデータSCDAT1を上階層の機密レベルAに応じた画像処理に変更する特定のID解除キーコードを登録するか否かを判定する。このステップSC2の判定が、特定のID解除キーコードを登録するYESの場合には、ステップSC3において、ID解除キーコードを登録する。

【0050】それから、ステップSC4において、データ管理部22のID付与部22aにより付与された機密レベルA, Bに応じたIDコード通りのパーソナルコンピュータp c A～p c D宛のeメールアドレスをメール作成部24によって作成する。この場合、下階層の機密レベルBは、パーソナルコンピュータp c Cのみとなるので、このパーソナルコンピュータp c Cのeメールアドレスのみがメール作成部24によって作成される。

【0051】その後、上記ステップSC2の判定が特定のID解除キーコードを登録しないNOの場合と同様に、ステップSC5において、スキャンデータSCDAT1、各パーソナルコンピュータp c C宛のeメールアドレス、およびID解除キーコードなどのデータをキャナ部本体10内の記憶部に記憶し、終了する。

【0052】—パーソナルコンピュータからキャナ装置にアクセスする場合の説明ー

パーソナルコンピュータp c A～p c Dからキャナ装置1にアクセスする場合には、先ず、図18のフローチャートのステップSD1において、パーソナルコンピュータp c A～p c D宛にスキャンデータSCDAT1, SCDAT2の各階層の機密レベルA, Bに応じたIDコード、IDBコードが添付されたeメールを受信するまで待機した後、ステップSD2で、図13に示すように、スキャンデータSCDAT1またはSCDAT2を選択し、その選択されたスキャンデータSCDAT2(SCDAT1)のダウンロードを要求する。

【0053】次いで、ステップSD3において、各パーソナルコンピュータp c A～p c Dの操作画面上でIDコードを入力したか否かを判定し、IDコードが入力されないNOの場合には、スキャンデータSCDAT2をダウンロードさせることなく終了する。

【0054】一方、上記ステップSD3の判定が、IDコードが入力されたYESの場合には、ステップSD4において、各パーソナルコンピュータp c A～p c Dの

50

12

IDレベルをデータ管理部22で解析した後、ステップSD5で、スキャンデータSSCDAT2に対し上階層に応じた機密レベルAの画像処理、または下階層に応じた機密レベルBの画像処理をそれぞれ施す。具体的には、機密レベルAの画像処理が施されるパーソナルコンピュータp c A, p c B, p c Dでは、スキャンデータSCDAT2が原稿のまま画像処理される。一方、機密レベルBの画像処理が施されるパーソナルコンピュータp c Cでは、スキャンデータSCDAT2の文字情報(電話番号およびeメールアドレス)を削除する画像処理が施される。

【0055】その後、ステップSD6において、各パーソナルコンピュータp c A～p c Dの画面上に機密レベルA, Bに応じて画像処理されたスキャンデータSCDAT2をダウンロードする。

【0056】—パーソナルコンピュータからキャナ装置にID解除キーコードの有無でアクセスする場合の説明ー

パーソナルコンピュータp c A～p c Dからキャナ装置1にID解除キーコードの有無でアクセスする場合には、先ず、図19のフローチャートのステップSE1において、パーソナルコンピュータp c A～p c D宛にスキャンデータSCDAT1, SCDAT2の各階層の機密レベルA, Bに応じたIDAコード、IDBコードが添付されたeメールを受信するまで待機した後、ステップSE2で、スキャンデータSCDAT1またはSCDAT2を選択し、その選択されたスキャンデータSCDAT2(SCDAT1)のダウンロードを要求する。

【0057】次いで、ステップSE3において、各パーソナルコンピュータp c A～p c Dの操作画面上でIDコードが入力されたか否かを判定し、IDコードが入力されないNOの場合には、スキャンデータSCDAT1をダウンロードさせることなく終了する。一方、上記ステップSE3の判定が、IDコードが入力されたYESの場合には、ステップSE4において、各パーソナルコンピュータp c A～p c DのIDレベルをデータ管理部22で解析する。

【0058】その後、ステップSE5で、各パーソナルコンピュータp c A～p c Dの操作画面上でID解除キーコードが入力されたか否かを判定し、ID解除キーコードが入力されないNOの場合には、ステップSE6において、スキャンデータSCDAT1に対し上階層の機密レベルAおよび下階層の機密レベルBにそれぞれ応じた画像処理1を施す。具体的には、機密レベルAの画像処理では、スキャンデータSCDAT1の第1ページ～第4ページを原稿のまま画像処理する。一方、機密レベルBの画像処理では、スキャンデータSCDAT1の第1ページ、第2ページおよび第4ページを削除して第3ページのみを原稿のまとめる画像処理を施す。

【0059】一方、ステップSE5の判定が、ID解除

(8)

13

キーコードが入力されたYESの場合には、ステップSE7において、スキャンデータSCDAT1に対し下階層の機密レベルBを上階層の機密レベルAに変更する画像処理2を施す。つまり、スキャンデータSCDAT1に対し上階層の機密レベルAに応じた画像処理を施すのはもちろんのこと、下階層の機密レベルBに応じた画像処理を施したスキャンデータSCDAT1を上階層の機密レベルAに応じた画像処理に変更する。具体的には、図14に示すように、機密レベルBの画像処理をID解除キーコードによって変更したスキャンデータSCDAT1では、上階層の機密レベルとなる第1ページ、第2ページおよび第4ページに対し社外秘などのウォータマークを挿入し、第1ページ～第4ページを削除しない画像処理を施す。

【0060】しかる後、ステップSE8において、各パーソナルコンピュータpca～pcDの画面上に機密レベルA、B、またはID解除キーコードにより上階層に変更した機密レベルに応じて画像処理されたスキャンデータSCDAT1をダウンロードする。

【0061】このように、スキャンデータの一部分のみを機密とする場合には、下階層の機密レベルBに応じてIDBが付与されたパーソナルコンピュータpcCにおいて、下階層の機密レベルBに応じた画像処理を施したスキャンデータSCDAT1、SCDAT2、具体的には、スキャンデータSCDAT1では第1ページ、第2ページおよび第4ページを削除して第3ページのみを原稿のままする画像処理を、スキャンデータSCDAT2では文字情報（電話番号およびeメールアドレス）を削除する画像処理をそれぞれ施したスキャンデータがLANによって共有されることになる。これにより、下階層の機密レベルBとなるパーソナルコンピュータpcCでは、上階層の機密レベルAの機密部分（スキャンデータSCDAT1の第1ページ、第2ページおよび第4ページ、並びにスキャンデータSCDAT2の文字情報）を除くスキャンデータがLANによって共有され、上階層の機密レベルAに触れない下階層の機密レベルB（必要最小限の情報）のスキャンデータを共有することができる。

【0062】一方、上階層の機密レベルAのスキャンデータは、その上階層の機密レベルAに応じたIDAが付与されたパーソナルコンピュータpca、pcB、pcDにおいてのみ共有され、そのスキャンデータの機密性および著作権を円滑に保護することができる。

【0063】しかも、4枚の原稿からなるスキャンデータSCDAT1に対し上階層の機密レベルAの第1、第2および第4ページを削除して下階層の機密レベルBの第3ページのみとするページ制御の画像処理を施すことで、上階層の機密レベルAとなる原稿の第1、第2および第4ページの機密性を円滑に保護することができる。さらに、下階層の機密レベルBのスキャンデータSCD

(8)

14

AT2に対し原稿の特定部分の文字情報（電話番号およびeメールアドレス）を削除する画像処理を施すこと、悪用され易い文字情報を削除したスキャンデータが共有され、上階層の機密レベルAとなる電話番号やeメールアドレスなどの知られたくない文字情報の機密性を円滑に保護することができる。その上、スキャンデータSCDAT1、SCDAT2のデータ量が共に少なくなつてダウンロードの高速化を図ることができる。

【0064】また、下階層の機密レベルBに応じて画像処理が施されたスキャンデータを上階層の機密レベルAに応じた画像処理に変更するように下階層の機密レベルBの設定を上階層の機密レベルへ移行可能に解除する解除部22cを備え、パーソナルコンピュータpcCにおいて、LANを介してスキャナ装置1から送信された特定のID解除キーコードを入力することによって下階層の機密レベルBの設定解除が行われるので、パーソナルコンピュータpcCにおいて上階層の機密レベルに応じたスキャンデータが取り出され、必要に応じて上階層の機密レベルAのスキャンデータを共有することができる。しかも、取得した上階層の機密レベルAのスキャンデータを、再び他のパーソナルコンピュータ（上階層の機密レベルAのIDが付与されていないパーソナルコンピュータ）などに対し制限を加えた状態、つまり下階層の機密レベルBのIDを付与した状態で、ダウンロード可能にスキャンデータを出力することもできる。

【0065】なお、本発明は上記実施形態に限定されるものではなくその他種々の変形例を包含するものである。たとえば、上記実施形態では、パーソナルコンピュータpcCにLANを介してスキャナ装置1から送信された特定のID解除キーコードを入力させることによって下階層の機密レベルBの設定解除を行えるようになつたが、特定のID解除キーがスキャナ部本体の操作表示部の液晶モニタ画面上に表示されるようにしても良い。この場合、下階層の機密レベルのIDが付与されたパーソナルコンピュータにおいて、スキャナ部本体の操作表示部（液晶モニタ画面）に表示された特定のID解除キーコードを入力することで、必要に応じて上階層の機密レベルのスキャンデータを共有することができることになる。

【0066】また、本実施形態では、機密レベルを上階層と下階層との2階層に分けたが、3階層以上の機密レベルに分けられていてもよい。その場合、上位の階層に1階層ずつ移行可能とするID解除キーコードであつてもよいのはもちろんのこと、上位の階層に2階層以上ずつ移行可能とするID解除キーコードであつてもよい。

【0067】

【発明の効果】以上のように、本発明では、スキャンデータに対し階層の異なる機密レベルに応じた画像処理をそれぞれ施してネットワーク上で共有することで、下階

(9)

15

層の機密レベルのネットワーク端末において上階層の機密レベルの機密部分を除く下階層の機密レベルのスキャンデータをネットワーク上で共有することができる一方、上階層の機密レベルに応じたネットワーク端末においてのみ上階層の機密レベルのスキャンデータを共有し、そのスキャンデータの機密性および著作権を円滑に保護することができる。

【0068】特に、下階層のスキャンデータに対する画像処理の具体的な施し方として、原稿の色情報を変更する画像処理を施すことで、下階層の機密レベルのネットワーク端末において、原画をカラーからモノクロなどに変更したスキャンデータを共有させ、上階層の機密レベルとなる原画の機密性および著作権を円滑に保護することができる上、スキャンデータのデータ量を少なくしてダウンロードを高速で行うことができる。

【0069】これに対し、下階層の機密レベルのスキャンデータに対し原稿の特定部分の文字データ情報を削除する画像処理を施すことで、下階層の機密レベルのネットワーク端末において、悪用され易い住所、氏名、電話番号などの文字データ情報を削除したスキャンデータを共有させ、知られたくない文字データ情報の機密性を円滑に保護することができる。

【0070】また、下階層の機密レベルのスキャンデータに対し原稿の解像度を低くする画像処理を施すことで、下階層の機密レベルのネットワーク端末において、原画の解像度を低くしたスキャンデータを共有させ、原画の機密性および著作権を円滑に保護することができる上、スキャンデータのデータ量の減少によってダウンロードの高速化を図ることができる。

【0071】しかも、下階層の機密レベルのスキャンデータに対し原稿の特定部分にウォータマークを挿入する画像処理を施すことで、下階層の機密レベルのネットワーク端末において、社外秘などのウォータマークを挿入したスキャンデータを共有させ、ダウンロードした社外秘付きの原稿に対し個人レベルで機密性を喚起させて、上階層の機密レベルとなる原画の機密性および著作権を各人によって保護することができる。

【0072】さらに、複数枚の原稿からなるスキャンデータに対し上階層の機密レベルとなるページを削除する画像処理を施すことで、下階層の機密レベルのネットワーク端末において、下階層の機密レベルのページのみとなるスキャンデータを共有させ、上階層の機密レベルとなる原画の機密性を円滑に保護することができる上、スキャンデータのデータ量の減少によってダウンロードの高速化を図ることができる。

【0073】特に、下階層の機密レベルのネットワーク端末において、解除手段により機密レベルの設定を上位の階層へ移行可能に解除することで、必要に応じて原画などの所望の情報を取り出して上位階層の機密レベルのスキャンデータを共有することができる。

16

【0074】特に、機密レベルを上位へ移行可能に解除する具体的な設定の仕方として、機密レベルの設定解除を行う特定のID解除キーを、下階層の機密レベルに応じたネットワーク端末に対しネットワークを介して送信することで、下階層の機密レベルのネットワーク端末において、必要に応じて上位階層の機密レベルのスキャンデータを共有することができ、取得した上位階層の機密レベルのスキャンデータを、再び他のネットワーク端末に対し下階層の機密レベルのIDを付与してダウンロード可能に出力することができる。

【0075】これに対し、特定のID解除キーをスキャナ装置本体の表示部に表示するようにすることで、下階層の機密レベルのネットワーク端末において、必要に応じて原画などの所望の情報を共有することができる上、他のネットワーク端末に対し再び制限を加えた状態でダウンロード可能に出力することができる。

#### 【図面の簡単な説明】

【図1】本発明の実施形態に係るスキャナ装置の概略構成図である。

【図2】4枚の原稿からなるスキャンデータSCDAT1を示す図である。

【図3】スキャンデータSCDAT1に対しページ制御の画像処理を施す操作を行う場合の操作表示部の液晶モニタ画面を示す図である。

【図4】スキャンデータSCDAT1の各階層の機密レベルA, Bに応じたIDコードおよびID解除キーコードをパーソナルコンピュータに対し付与する場合の説明図である。

【図5】スキャンデータSCDAT1のヘッダーを登録する場合の説明図である。

【図6】スキャンデータSCDAT1に対しページ制御の画像処理を施してヘッダ登録する場合の説明図である。

【図7】スキャンデータSCDAT2を示す図である。

【図8】文字情報削除の画像処理が施されたスキャンデータSCDAT2を示す説明図である。

【図9】スキャンデータSCDAT2の各階層の機密レベルA, Bに応じたIDコードをそれぞれ付与する場合の説明図である。

【図10】スキャンデータSCDAT2のヘッダーを登録する場合の説明図である。

【図11】スキャンデータSCDAT2に対し文字情報削除の画像処理を施してヘッダ登録する場合の説明図である。

【図12】機密レベルA, Bに応じたIDコード通りのパーソナルコンピュータp c A～p c D宛のeメールアドレスを作成する場合の説明図である。

【図13】パーソナルコンピュータの操作画面上においてスキャンデータSCDAT2を選択する場合の説明図である。

(10)

17

【図14】機密レベルBの画像処理をID解除キーコードによって変更する画像処理が施されたスキャンデータSCDAT1を示す図である。

【図15】スキャンデータSCDAT1を記憶する場合の制御部による制御の手順を示すフローチャート図である。

【図16】スキャンデータSCDAT2を引き続いで記憶する場合の制御部による制御の手順を示すフローチャート図である。

【図17】スキャンデータSCDAT1に特定のID解除キーコードを付与する場合の制御部による制御の手順を示すフローチャート図である。

【図18】パソコンからスキャナ装置にアクセスする場合の制御部による制御の手順を示すフローチャート図である。

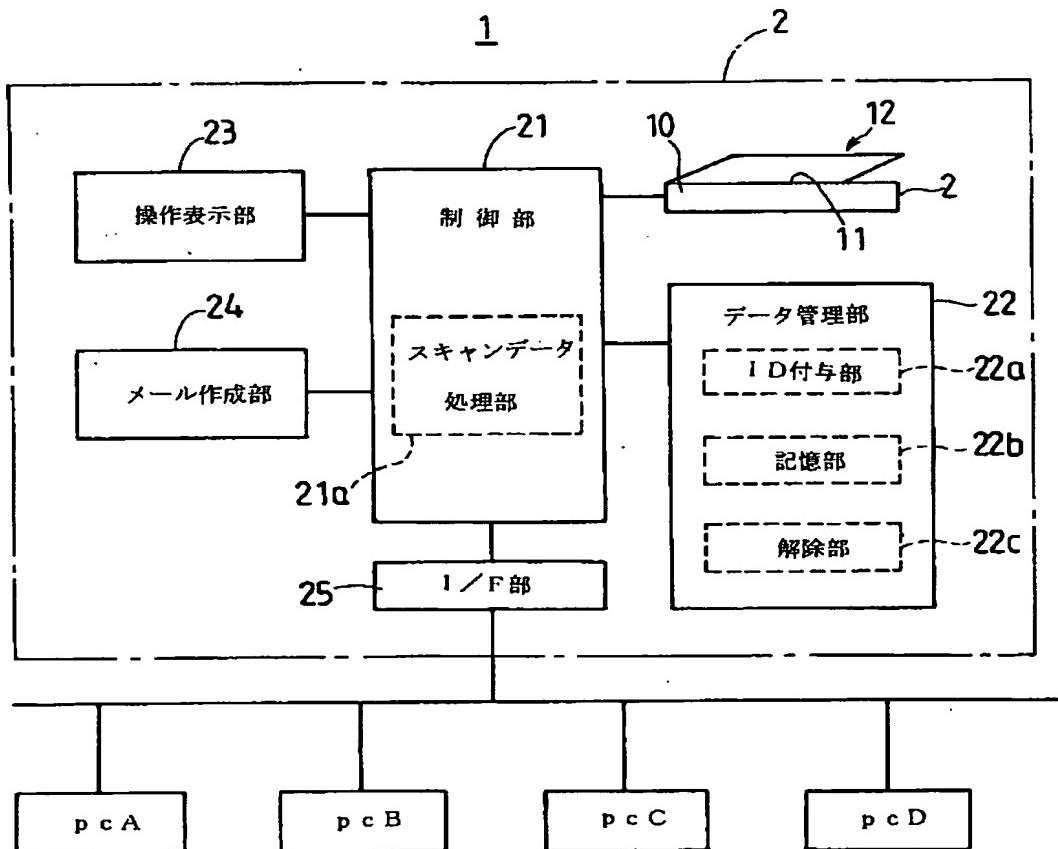
18

【図19】パソコンからスキャナ装置にID解除キーコードの有無でアクセスする場合の制御部による制御の手順を示すフローチャート図である。

【符号の説明】

1	スキャナ装置
10	スキャナ部本体（スキャナ装置本体）
11	原稿台
21a	スキャンデータ処理部（画像処理手段）
22a	ID付与部（ID付与手段）
22c	解除部（解除手段）
23	表示モニタ画面（表示部）
A, B	機密レベル
SCDAT1, SCDAT2	スキャンデータ
p c A ~ p c D	パソコン（ネットワーク端末）

【図1】



【図9】

データ : SCDAT2  
IDA : XOOOOO

データ : SCDAT2  
IDB : OOXxxx

(11)

【図2】

## SCDAT 1

第1ページ  
XXXXXX  
XXXXXX  
XXXXXX

A

第2ページ  
XXXXXX  
XXXXXX  
XXXXXX

A

第3ページ  
XXXXXX  
XXXXXX  
XXXXXX

B

第4ページ  
XXXXXX  
XXXXXX  
XXXXXX

A

## File Name : S C D A T 2

e メールアドレス :

I D :

解除キーコード:  ダウンロード

【図13】

【図3】

## 操作パネル

File Name : S C D A T 1  
ページ制御階層レベル  
第1ページ: A  
第2ページ: A  
第3ページ: A, B  
第4ページ: A

→ 23a I D設定

I DA : XXXOOO	解除キー: なし
I DB : OXOXOX	解除キー: OOXXXX

【図4】

【図5】

ヘッダー		スキャンデータ		
データ名	レベル	I D	解除キーコード	e メールアドレス
SCDAT 1	A	XXXOOO	-	pcA@sharp.co.jp
	A	XXXOOO	-	pcD@sharp.co.jp
	A	XXXOOO	-	pcB@sharp.co.jp
	B	OXOXOX	OXXXOO	pcC@sharp.co.jp

(12)

【図6】

データ名	レベル	画像処理
------	-----	------

SCDAT 1	A	ページ制御	第1, 2, 3, 4ページ
	B	ページ制御	第3ページ

【図7】

SCDAT 2

社員データ  
住所：大和郡山市美濃庄町492  
氏名：早川 太郎  
電話番号：0743-55-7862  
eメールアドレス：tarō@sharp.co.jp

SCDAT 2

社員データ  
住所：大和郡山市美濃庄町492  
氏名：早川 太郎  
電話番号：  
eメールアドレス：

【図10】

ヘッダー	スキャンデータ				
データ名	レベル	ID	解除キーコード	eメールアドレス	
SCDAT 1	A	x00000	-	pcA@sharp.co.jp	
	A	x00000	-	pcD@sharp.co.jp	
	A	x00000	-	pcB@sharp.co.jp	
	B	00xxxx	-	pcC@sharp.co.jp	

(13)

【図11】

データ名	レベル	画像処理
------	-----	------

SCDAT2	A	文字情報削除なし
	B	文字情報削除（電話番号・eメールアドレス）

【図12】

<ID送信>

File Name : S C D A T 1

IDレベルA :

pcA@sharp.co.jp  
pcB@sharp.co.jp  
pcD@sharp.co.jp

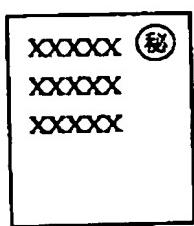
IDレベルB :

pcC@sharp.co.jp

メール送信

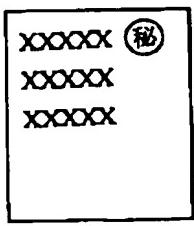
【図14】

第1ページ



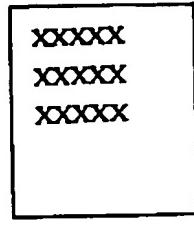
A

第2ページ



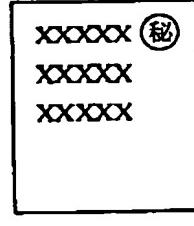
A

第3ページ



A, B

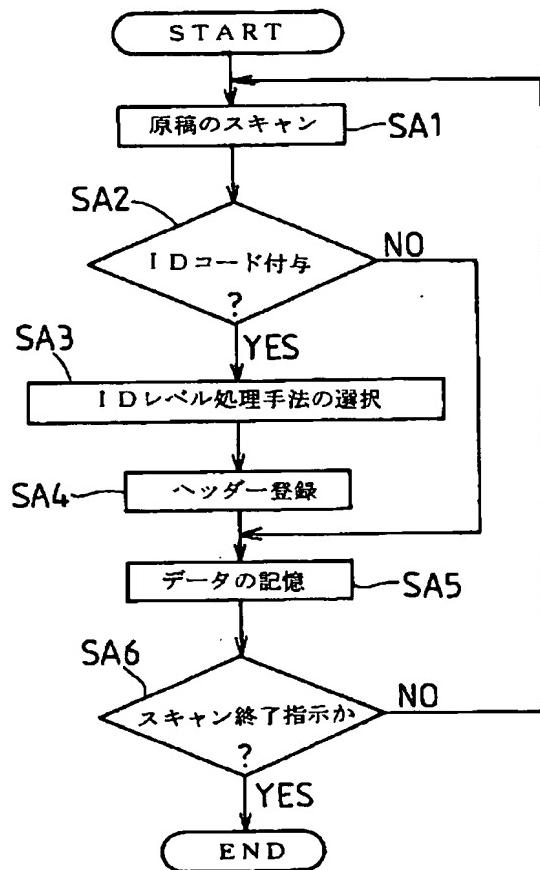
第4ページ



A

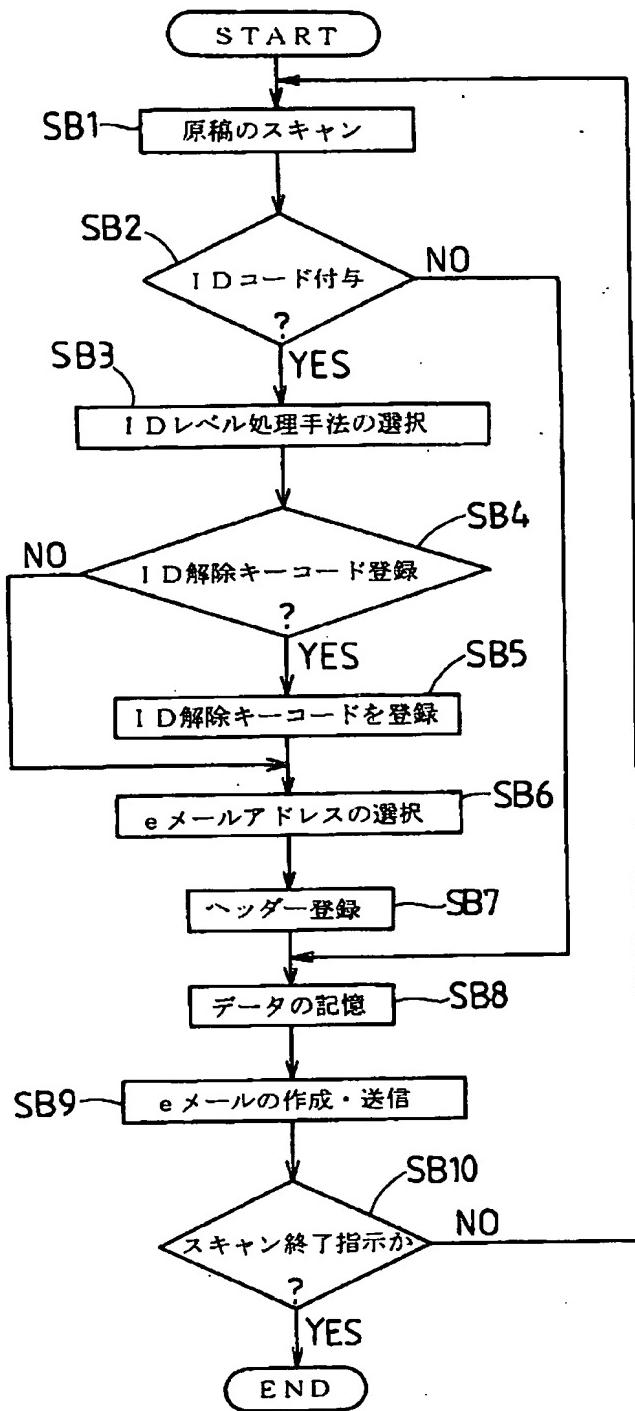
(14)

【図15】



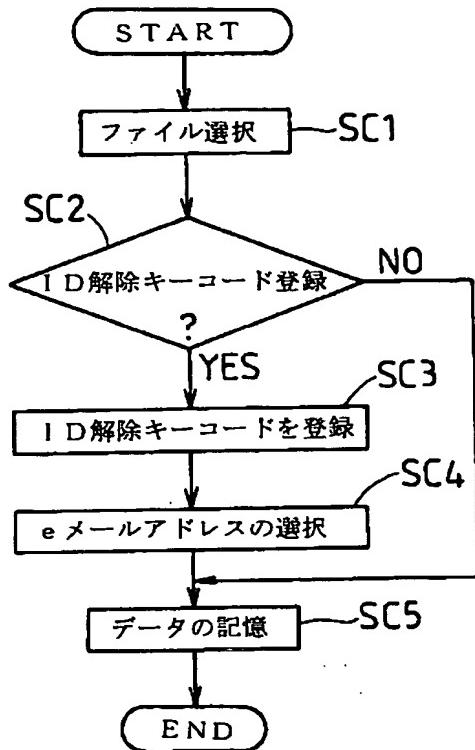
(15)

【図16】



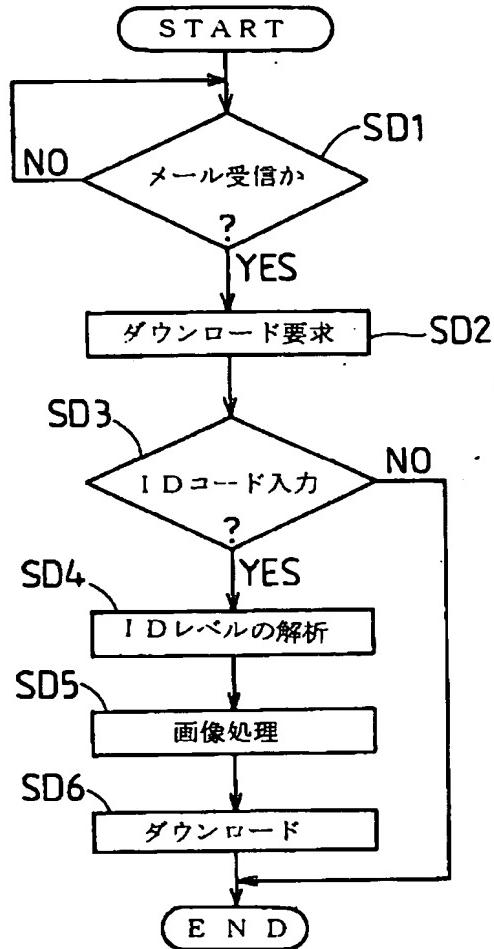
(16)

【図17】



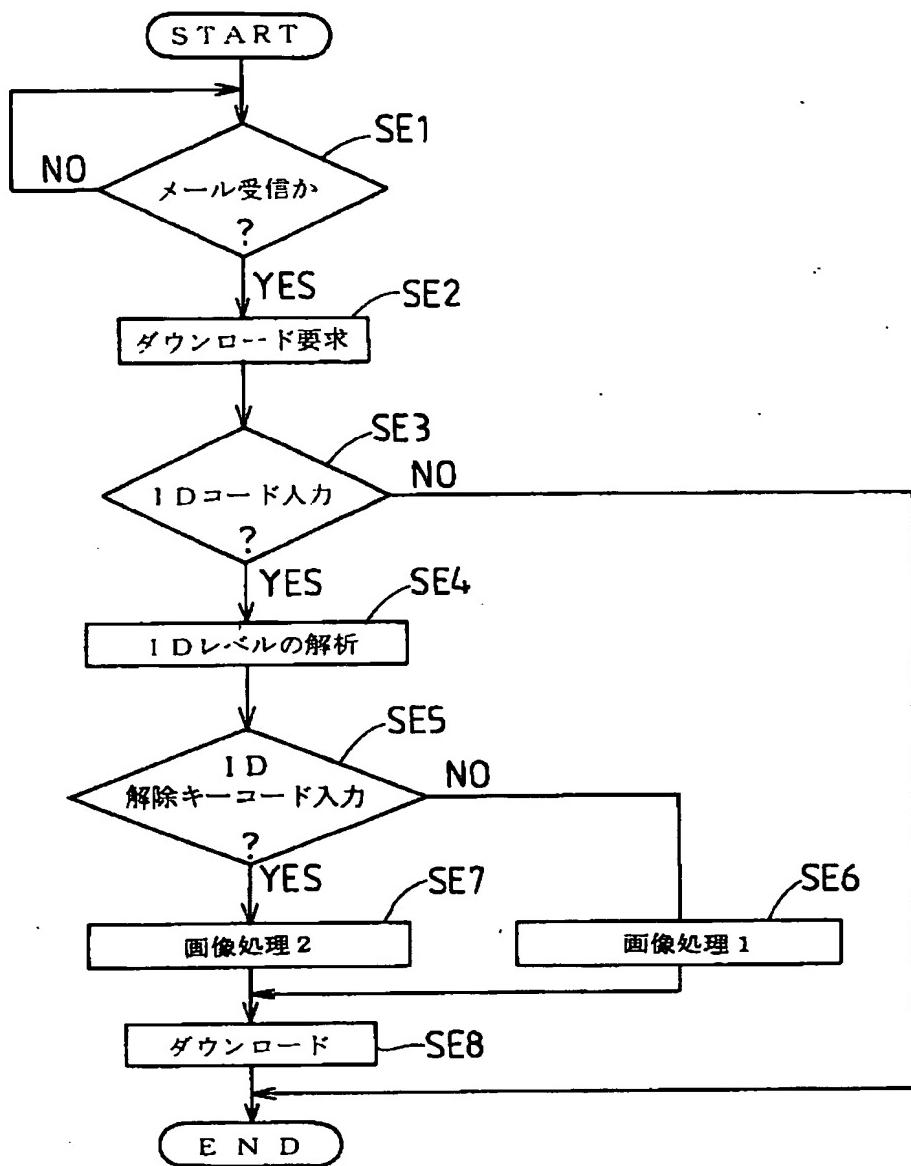
(17)

【図18】



(18)

【図19】



フロントページの続き

(72)発明者 森 かおり  
 大阪府大阪市阿倍野区長池町22番22号 シ  
 ャープ株式会社内

(19)

F ターム(参考) 5B057 AA11 BA02 BA23 CA01 CA08  
CA12 CA16 CB01 CB08 CB12  
CB16 CB19 CD05 CE08 CE17  
CE20 CG07 CH18  
5B085 AA08 AE04 AE06  
5C062 AA05 AA14 AA35 AB17 AB20  
AB25 AB38 AB42 AC08 AC21  
AC24 AC43 AE15 AF00 BA00  
5C075 CD05 EE01 EE02  
5C076 AA03 AA14 AA22 AA26 BA06  
CA02 CB05